

WE CLAIM:

1. A security envelope, comprising:

a barcode in a two-dimensional symbology located on the security envelope, the barcode encoding:

5 a public component, the public component comprising a public digital mail identification and a digital signature signed by the sender encrypted by the private key of the sender; and

a private component, the private component comprising a private digital mail identification and a digital signature signed by the sender encrypted by the public key of the receiver.

2. The security envelope as in claim 1, where the two-dimensional symbology is PDF-417.

3. The security envelope as in claim 2, wherein the barcode further encodes return address information.

4. The security envelope as in claim 2, wherein the barcode further encodes information relating to the physical characteristics of the security envelope.

5 The security envelope as in claim 4, wherein the information relating to the physical characteristics of the security envelope include at least one of: (a) the date the security envelope was sealed; (b) the size of the security envelope; and (c) the weight of the security envelope.

6. The security envelope as in claim 2, wherein the barcode further encodes stamp information.

7. The security envelope as in claim 2, wherein the security envelope further comprises a physical authentication identification and wherein the barcode further comprises a digital representation of the physical authentication identification.

8. The security envelope as in claim 7, where the physical authentication identification comprises an optically clear epoxy with air bubbles suspended therein.

9. The security envelope as in claim 7, where the physical authentication identification comprises a cloth made from non-woven 40 micron diameter polymer fibers.

10. A method for securing the mails, comprising:

(1) producing a digital mail identification that encodes physical identification information of a security envelope into a barcode in a two-dimensional symbology; wherein the digital mail identification comprises:

(a) a public component, the public component comprising a public digital mail identification and a digital signature signed by the sender encrypted by the private key of the sender; and

(b) a private component, the private component comprising a private digital mail identification and a digital signature signed by the sender encrypted by the public key of the receiver;

(2) applying the digital mail identification to the security envelope.

11. The method as in claim 10, where the two-dimensional symbology is PDF-417.

12. The method as in claim 11, wherein the physical identification information comprises return address information.

13. The method as in claim 11, wherein the physical identification information comprises information relating to the physical characteristics of the security envelope.

14. The method as in claim 13, wherein the information relating to the physical characteristics of the security envelope include at least one of: (a) the date the security envelope was sealed; (b) the size of the security envelope; and (c) the weight of the security envelope.

15. The method as in claim 11, wherein the physical identification information comprises stamp information.

16. The method as in claim 11, where the physical identification information comprises an optically clear epoxy with air bubbles suspended therein.

17. The method as in claim 11, where the physical identification information comprises a cloth made from non-woven 40 micron diameter polymer fibers.

18. The method as in claim 11, further comprising:

measuring the physical identification information;

decoding the digital mail identification;

comparing the measured physical identification information with the decoded digital mail identification.

19. The method as in claim 18, wherein at least one of the steps of (1) measuring the physical identification information, and (2) decoding the digital mail identification is accomplished using an optical scanner.

20. The method as in claim 19, wherein the step of comparing the measured physical
5 identification information with the decoded digital mail identification is accomplished using a mobile computer.

21. The method as in claim 19, further comprising:

transmitting the measured physical identification information and the decoded digital mail
identification to a wired computer network via a wireless medium.

22. The method as in claim 21, wherein the wired computer network is connected to the
Internet and the transmitting the identification data to a wired computer network via a wireless
medium uses a TCP/IP protocol.

23. A system of securing the mails, comprising:

(1) at least one security envelope, comprising

15 (a) a barcode in a two-dimensional symbology located on the security envelope,
the barcode encoding:

(i) a public component, the public component comprising a public
digital mail identification and a digital signature signed by the sender encrypted by the private key
of the sender; and

1002972 12345678901

(ii) a private component, the private component comprising a private digital mail identification and a digital signature signed by the sender encrypted by the public key of the receiver;

(2) at least one mobile computer, comprising:

- 5 (a) a bar code reader;
- (b) a physical authentication identifier reader;
- (c) a computer capable of comparing information obtained from the bar code reader and the physical authentication identifier reader;
- (d) a database capable of storing at least one public key and at least one private key;
- (e) a display; and
- (f) a printer.

24. The system as in claim 23, where the two-dimensional symbology is PDF-417.

25. The system as in claim 24, where the at least one security envelope further comprises an
15 optically clear epoxy with air bubbles suspended therein.

26. The system as in claim 24, where the at least one security envelope further comprises a cloth made from non-woven 40 micron diameter polymer fibers.

27. The system as in claim 24, further comprising:

a wired computer network capable of communication with the at least one mobile computers via a wireless medium.

28. The system as in claim 27, wherein the wired computer network is connected to the Internet using a TCP/IP protocol.